

(Eddie) Jae K. Kim (CA Bar No. 236805)  
**LYNCH CARPENTER, LLP**  
 117 East Colorado Blvd., Suite 600  
 Pasadena, CA 91105  
 Tel.: (626) 550-1250  
 ekim@lcllp.com

Gary F. Lynch (admitted *pro hac vice*)  
 Jamisen A. Etzel (admitted *pro hac vice*)  
 Nicholas A. Colella (admitted *pro hac vice*)  
**LYNCH CARPENTER, LLP**  
 1133 Penn Ave., 5th Floor  
 Pittsburgh, PA 15222  
 Tel.: (412) 322-9243  
 gary@lcllp.com  
 jamisen@lcllp.com  
 nickc@lcllp.com

Christian Levis (admitted *pro hac vice*)  
 Amanda Fiorilla (admitted *pro hac vice*)  
 Rachel Kesten (admitted *pro hac vice*)  
 Christopher Devivo (*pro hac vice* forthcoming)  
**LOWEY DANNENBERG, P.C.**  
 44 South Broadway, Suite 1100  
 White Plains, NY 10601  
 Tel: (914) 997-0500  
 Fax (914) 997-0035  
 clevis@lowey.com  
 afiorilla@lowey.com  
 rkestn@lowey.com  
 cdevivo@lowey.com

*Attorneys for Plaintiff and the Proposed Class*

**UNITED STATES DISTRICT COURT**  
**NORTHERN DISTRICT OF CALIFORNIA**

JANE DOE, individually and on behalf of all  
 others similarly situated,  
  
 Plaintiff,  
  
 v.  
  
 FULLSTORY, INC., META PLATFORMS,  
 INC., TIKTOK, INC., AND BYTEDANCE INC.  
  
 Defendant.

Case No.: 3:23-cv-00059-WHO

**AMENDED CLASS ACTION  
 COMPLAINT**

**JURY TRIAL DEMANDED**

Plaintiff Jane Doe (“Plaintiff”), individually and on behalf of all others similarly situated, asserts the following against Defendants FullStory, Inc. (“FullStory”), Meta Platforms, Inc. (f/k/a Facebook, Inc.) (“Meta”), TikTok, Inc. (f/k/a Musical.ly, Inc.) and ByteDance Inc. (collectively with TikTok, Inc., “TikTok”) based upon personal knowledge, where applicable, information and belief, and the investigation of counsel.

**SUMMARY OF ALLEGATIONS**

1. Hey Favor, Inc. (“Favor”) (formerly the “Pill Club”) is a combination telemedicine company and direct-to-consumer pharmacy that prescribes its patients birth control, emergency

1 contraception (e.g., morning-after-pills), STI test kits, acne medicine, and prescription-strength  
 2 retinol. Users can also purchase directly from Favor other menstrual care and sexual wellness  
 3 products, like condoms, lubrication, and pregnancy tests, and learn from medical information it  
 4 provides on health and wellness topics, like periods, skin conditions, and birth control. Visitors  
 5 access these services and products through Favor’s website at [www.heyfavor.com](http://www.heyfavor.com) and/or through  
 6 its mobile app (collectively, “the Favor Platform”).

7         2. Favor represents that its “digital primary care” platform is designed to “[m]ake  
 8 healthcare more accessible.” Favor is now available in 49 states and Washington, D.C. and its  
 9 website receives approximately 450,000 monthly visitors. Favor states that the Favor Platform has  
 10 allowed “3 million patients get access to birth control” to date.

11         3. Favor’s services are comprised of three main components: (1) its “Medical Team”  
 12 consisting of doctors and nurse practitioners who review users’ health history, evaluate their needs,  
 13 prescribe medications, and answer medical questions; (2) its “Pharmacy Team” comprised of  
 14 pharmacists and technicians who review and process medication orders; and (3) its “Patient Care  
 15 Team” who assist patients and personalize their care.

16         4. Customers must provide Favor with personally identifiable information (“PII”) (e.g.,  
 17 their names, email addresses, date of birth, place of residence, payment information, and health  
 18 insurance information) to use its telehealth platform. Favor also collects other identifiable  
 19 information from users, including their IP address, unique device information and identifiers, and  
 20 cookie data, which are used to track users across the internet.

21         5. Favor requires users to complete an “online consultation” that prompts users to  
 22 “[a]nswer . . . health questions” before they can receive medication. These questions are highly  
 23 sensitive and ask users directly for medical information, including their medical history. For  
 24 example, a patient visiting the Favor Platform for birth control is asked: (1) “what type of birth  
 25 control are you on?”; (2) “are you pregnant?”; (3) “how long has it been since you last gave birth?”;  
 26 (4) “how frequently would you like your period?”; (5) “are you taking hormones?”; (6) “do you  
 27 have any history of breast cancer?”; (7) “do you have high cholesterol medicine?”; and (8) “what  
 28 other medications are you on?” Users are required to answer similar, highly sensitive medical

1 questions about their health to obtain emergency contraception, acne medicine, and other treatment  
2 through the Favor Platform.

3 6. Favor also requires users from certain states, including those in Arkansas where  
4 Plaintiff resides, to complete a separate medical consultation over video chat prior to obtaining a  
5 prescription. During this consultation, a medical professional evaluates the user, prompting them to  
6 answer additional health questions, including those about the patient’s medication, medical history,  
7 and family health history.

8 7. Favor uses the answers to these questions to create a “digital health profile” for each  
9 user, which its Medical Team evaluates to determine treatment options and prescribe medication “if  
10 medically appropriate.” Favor’s Pharmacy Team sends any prescribed medication directly to the  
11 consumer, while its Patient Care Team continues to provide care after the medication is delivered  
12 by, among other things, answering questions the user may have about their medication or side  
13 effects.

14 8. Plaintiff and Class members provided their information to Favor based on the  
15 company’s repeated assurances that their intimate health data, PII, and other information would  
16 remain protected and confidential.

17 9. For instance, Favor represents that it “understand[s] that medical information about  
18 [users] and [their] health is personal” and that Favor is “committed to protecting it.”

19 10. Favor further states that it “takes the privacy of [users’] data and information very  
20 seriously” and that “[a]ll of the information [Favor] hold[s] is *treated as Protected Health*  
21 *Information (PHI).*” Accordingly, users’ “data is held to *even stricter privacy standard* than  
22 required by CCPA (Health Insurance Portability and Accountability Act (“HIPAA”), California  
23 Confidentiality of Medical Information Act, and Texas Medical Privacy Act, as some examples.)”

24 11. Favor goes on to ensure users that it is “required by law to make sure that medical  
25 information which identifies [users] is kept private (with certain exceptions).” These “exceptions”  
26 include the disclosure of users’ information to provide medical treatment (e.g., to doctors or nurses  
27 involved in the users’ treatment) and for payment processing (e.g., sending information about the  
28

1 users' prescriptions to the users' health plan in order to get paid) and does not include the disclosure  
2 of users' information for marketing, advertising, tracking, or analytics.

3 12. Favor also promises users that it does not disclose any "personal information" to  
4 third parties, including analytics companies, and expressly represents the only information it  
5 discloses is "aggregated" and "non-identifying" and that the third parties who receive it cannot use  
6 that information "for their commercial purposes." It even states in all bold and capital letters "WE  
7 DO NOT SELL OR MARKET YOUR PERSONAL INFORMATION AT ANY TIME."

8 13. Unbeknownst to Plaintiff and Class members, FullStory's, Meta's, and TikTok's  
9 (collectively "Defendants") technology was intentionally incorporated on Favor's Platform, through  
10 which Defendants intercepted users' health data and other highly sensitive information. Defendants  
11 intercepted at least users' prescription information (e.g., that they were prescribed birth control),  
12 answers to health questions (e.g., "what is your most recent blood pressure reading?" and "have you  
13 had or do you currently have breast cancer?"), medication side effects, allergies, age, and weight.  
14 In some instances, as is the case with FullStory, it intercepted *all of the users' interactions* on the  
15 Favor Platform (e.g., all individual clicks, keystrokes, and mouse movements), including their  
16 answers to highly sensitive medical questions.

17 14. This information was not aggregated or deidentified, nor were Defendants prohibited  
18 from using this information for their own benefit.

19 15. Plaintiff Jane Doe provided her information, including health data and PII in  
20 connection with obtaining prescriptions for birth control and emergency contraceptives, to Favor  
21 with the expectation that this information would remain confidential and private.

22 16. Defendants' interception of this information without consent constitutes an extreme  
23 invasion of Plaintiff's and Class members' privacy. Given the secret and undisclosed nature of  
24 Defendants' conduct, additional evidence supporting Plaintiff's claims, including the full extent of  
25 medical information Defendants intercepted, and how they used that information, will be revealed  
26 in discovery.

**PARTIES**

**A. Plaintiff**

17. **Plaintiff Jane Doe** is a resident of Hempstead County, Arkansas.

18. Plaintiff used the Favor Platform in or around the summer of 2021 to obtain medical services and products, including prescriptions for birth control, emergency contraception and condoms through the Favor Platform.

19. During the time Plaintiff used the Favor Platform, she maintained social media accounts with TikTok, Facebook, and Instagram. Plaintiff Jane Doe used the same device she used to access the Favor Platform to access these social media platforms.

20. To obtain her birth control prescriptions, Plaintiff Jane Doe was required to: (1) create a Favor account, (2) provide her PII, including her name, address, email, and health insurance information, and (3) provide her medical history and answer questions in response to Favor's health questionnaire, as described in paragraph 4-6, 13 above.

21. Plaintiff Jane Doe was also required to complete an additional medical consultation over video chat each time she wished to obtain a prescription. During this consultation, a medical professional evaluated Plaintiff Jane Doe over video and asked questions about her medical history, including what medications she takes and her family health history.

22. Plaintiff Jane Doe was required to answer additional health questions to obtain emergency contraception, including: (1) "what type of birth control do you use currently?"; (2) whether you are currently pregnant or breastfeeding; (3) what medications you take; (4) "do you have any medication allergies?"; and (5) "are you allergic to corn-containing products or food dye?".

23. Unbeknownst to Plaintiff Jane Doe, Defendants intercepted this information, including her PII, health data, prescription requests, and other activity across the Favor Platform.

24. Plaintiff Jane Doe did not consent to the interception of her data, which was never disclosed and directly contrary to the representations made by Favor.

**B. Defendants**

25. **Defendant Meta Platforms, Inc.** is a Delaware corporation with its principal place of business located in Menlo Park, California 94025.

1           26.     Meta at all times knew that the incorporation of its software into the Favor Platform  
2 would result in its interception of identifiable health information and other sensitive data.

3           27.     Meta, as the creator of its SDK and Meta Pixel, knew that it intercepted each of a  
4 user's interactions on the website or mobile application that incorporated this technology.

5           28.     Meta has consistently come under scrutiny for incorporating its technology on  
6 websites and applications that involve the transmittal of sensitive data, including health information,  
7 yet continues to do so.

8           29.     For instance, in February 2019, the *Wall Street Journal* published an in-depth  
9 analysis of Meta's collection of sensitive health information using its tracking technology from  
10 certain mobile applications. These reports led to a subsequent investigation by the Federal Trade  
11 Commission, who confirmed that Meta did in fact collect sensitive health information from a  
12 popular women's health app, including pregnancy data, between June 2016 to February 2019. It also  
13 confirmed that Meta went on to use this information for its own research and development. The  
14 New York State Department of Financial Services conducted a similar investigation of Meta and  
15 reached a similar conclusion, including finding that Meta did not take sufficient steps or precautions  
16 to prevent its interception of this kind of information or its use for commercial purposes.

17           30.     Further, since at least 2016, Meta has allowed granular ad targeting based on  
18 sensitive information collected or received about individuals, including relating to at least breast  
19 feeding, ethnicities, religious beliefs, and income levels.

20           31.     Despite this, it was not until November 9, 2021, that Meta acknowledged its use of  
21 data to target users based on "sensitive" topics, including "health" and how that was problematic.  
22 While Meta stated that it would remove this functionality in part, it later clarified that the change  
23 was limited to individuals' interactions with "content" on the Facebook platform (i.e., the "Detailed  
24 Targeting" option on Facebook) and ***did not apply to*** data intercepted through Meta Pixel or SDK  
25 or collected through other means. Thus, advertisers were still permitted to use "website custom  
26 audiences" and "lookalike" audiences to target users based on the information Meta intercepted  
27 through Meta Pixel and its SDK.  
28

1           32. Further, Meta has acknowledged its interception of sensitive data, including health  
2 information, in public statements highlighting its efforts to develop a “Health Terms Integrity  
3 System” intended to filter out this type of information and prevent them from entering Meta’s  
4 system.

5           33. However, independent investigations have confirmed these data filtration systems  
6 are not successful at preventing the interception of health data. For instance, researchers at *The*  
7 *Markup* found while investigating the use of the Meta Pixel on abortion-related websites that Meta’s  
8 purported “filtering” system failed to discard even the most obvious forms of sexual health  
9 information, including URLs that included the phrases “post-abortion” “i-think-im-pregnant” and  
10 “abortion-pill.”

11           34. Meta’s own employees have confirmed the same, admitting that Meta lacks the  
12 ability to prevent the collection of sensitive health data or its use in ads. For example, Meta engineers  
13 on the ad and business product team wrote in a 2021 privacy overview “We do not have an adequate  
14 level of control and explainability over how our systems use data, and thus we can’t confidently  
15 make controlled policy changes or external commitments such as ‘we will not use X data for Y  
16 purpose.’”

17           35. Meta did not take any steps to prevent Favor from using its technology on the Favor  
18 Platform or to prevent its interception and use of Favor users’ sensitive health data—like answers  
19 to health questions to obtain birth control.

20           36. As such, Meta’s conduct was intentional despite knowing the privacy violations it  
21 caused to Plaintiff and Class members.

22           37. **Defendant TikTok, Inc.** is a California corporation with its principal place of  
23 business located in Culver City, California.

24           38. **Defendant ByteDance Inc.** is a Delaware corporation with its principal place of  
25 business located in Mountain View, California. Upon information and belief, Defendant  
26 TikTok, Inc. and ByteDance Inc. do not operate as independent corporate entities, but rather  
27 function as satellite offices of the China-headquartered company ByteDance Technology Co. Ltd.  
28



1           39.     Since its founding, TikTok has come under scrutiny for the types of data it collects,  
2 stores, and shares, ranging from government fines over collecting children’s data to whether the app  
3 itself poses a national security risk for who it shares data with.

4           40.     TikTok, as the creator of the TikTok Pixel, knew that it intercepted each of a user’s  
5 interactions on the website or mobile application in which it is incorporated including those like the  
6 Favor Platform, which involve sensitive medical information.

7           41.     TikTok’s Pixel has come under intense scrutiny recently for its interception and  
8 collection of health data. A December 13, 2022 article by *The Markup* detailed these concerns,  
9 specifically highlighting the TikTok Pixel’s presence on the Favor Platform as an example.

10          42.     TikTok has not denied that it intercepts and collects users’ sensitive medical data or  
11 that it uses that data for commercial purposes. Rather, when pressed by journalists from Consumer  
12 Reports about its concerning practice of collecting health information, TikTok responded only that  
13 it “continuously work[s] with [its] partners to avoid inadvertent transmission of such data.”

14          43.     TikTok did not take any steps to prevent Favor from using its technology on the  
15 Favor Platform or to prevent its interception and use of Favor users’ sensitive data.

16          44.     As such, TikTok’s conduct was intentional despite knowing the privacy violations it  
17 caused to Plaintiff and Class members.

18          45.     **Defendant FullStory, Inc.** is a Delaware corporation with its principal place of  
19 business at 1745 Peachtree Street NE, Suite G, Atlanta, Georgia 30309.

20          46.     FullStory is well aware of the privacy concerns arising out of its tracking technology,  
21 including its session replay software.

22          47.     For example, a 2017 report from researchers at Princeton University found  
23 Walgreens.com’s use of session replay code was leaking website visitors’ medical conditions and  
24 prescriptions to FullStory. Because users’ names had been leaked earlier in website sessions,  
25 FullStory was able to link users’ identities to the medicine that they were prescribed.

26          48.     This occurred despite Walgreens using additional manual redaction tools to keep  
27 website visitors’ information private. In response to the discovery, Walgreens stopped using  
28



1 FullStory “out of an abundance of caution.” FullStory, on the other hand, took no affirmative steps  
2 to prevent its interception and identification of users through this software.

3 49. Other companies likewise denounced FullStory’s session replay software after  
4 finding out FullStory obtained credit card information through its incorporation. For example,  
5 clothing company Bonobos.com, announced that “We eliminated data sharing with FullStory in  
6 order to evaluate our protocols and operations with respect to their service. We are continually  
7 assessing and strengthening systems and processes in order to protect our customers’ data.”

8 50. Accordingly, FullStory understands that its software intercepts highly sensitive data,  
9 including health and medical information when used on a website or application like the Favor  
10 Platform, and that it would continue to do so as long as it remained installed.

11 51. FullStory did not take any steps to prevent Favor from using its technology on the  
12 Favor Platform or to prevent its interception and use of Favor users’ sensitive health data—like  
13 answers to health questions to obtain birth control.

14 52. As such, FullStory’s conduct was intentional despite knowing the privacy violations  
15 it caused to Plaintiff and Class members.

### 16 **JURISDICTION AND VENUE**

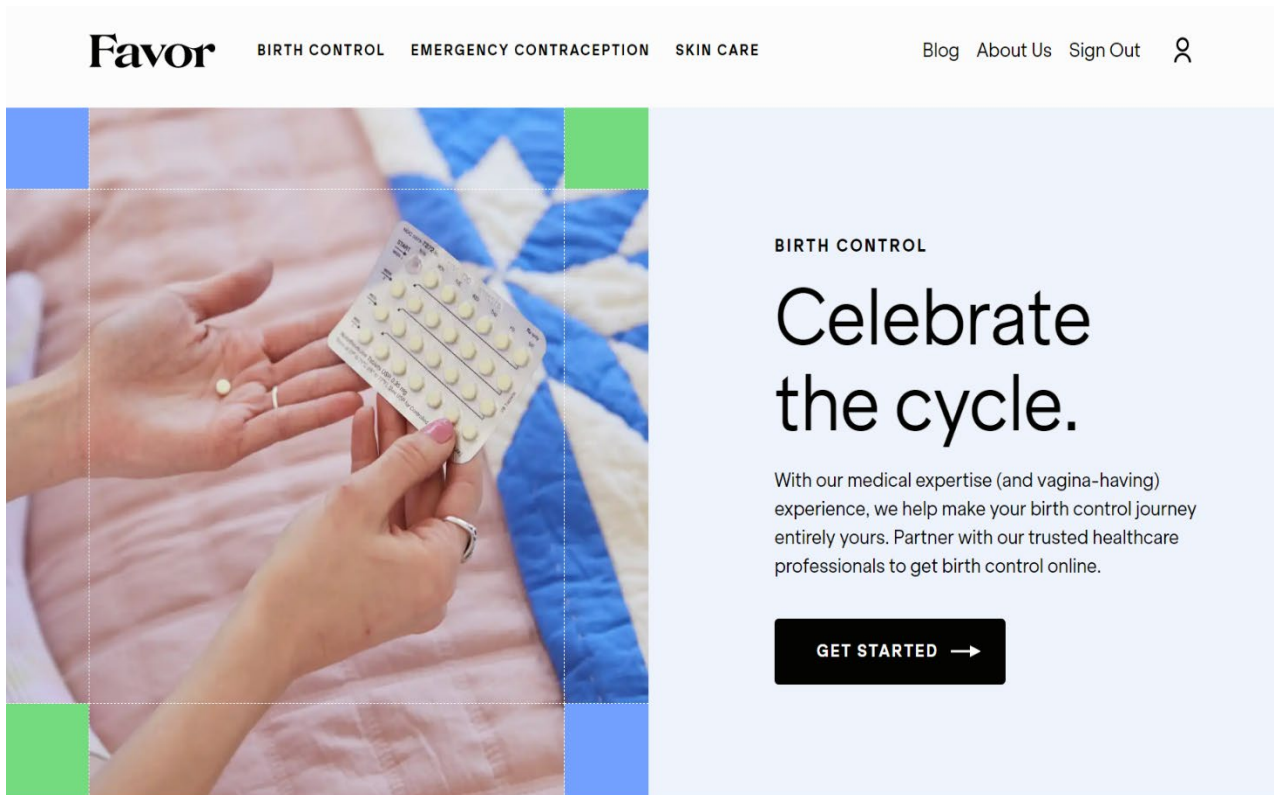
17 53. This Court has jurisdiction over the subject matter of this action pursuant to 28 U.S.C.  
18 § 1332(d), because the amount in controversy for the Class exceeds \$5,000,000 exclusive of interest  
19 and costs, there are more than 100 putative members of the Classes defined below, and a significant  
20 portion of putative Class members are citizens of a state different from the Defendants.

21 54. This Court also has subject matter jurisdiction over this action pursuant to 28 U.S.C.  
22 § 1332(a) because the amount in controversy in this case exceeds \$75,000 and this action is between  
23 citizens of different states.

24 55. This Court has personal jurisdiction over Meta because its principal place of business  
25 is in California. Meta is also subject to specific personal jurisdiction in this State because a  
26 substantial part of the events and conduct giving rise to Plaintiff’s claims occurred in this State,  
27 including Meta’s collection of Plaintiff’s sensitive health data from the Favor Platform and use of  
28 that data for commercial purposes.



62. As the company began to expand its product offerings to skincare, menstrual products, and sexual wellness products, it rebranded itself as Hey Favor in the Spring of 2022. Now, under the more “approachable” name Hey Favor, the company has positioned itself as the go-to, “cool” provider of reproductive health medications for the Gen Z customer base.



63. Today, Favor’s mission is “to create a new kind of healthcare for women and people who menstruate” through its “developed [] coalition of medical professionals, pharmacists, patient care experts, policy experts, and many more people to bring you the quality of care you deserve.” Favor touts itself as providing “digital care, prescriptions and products for a better wellbeing” using “U.S. licensed medical providers,” being a “licensed pharmacy” and “accepting most insurance.”

64. Favor’s products cover a wide range of healthcare services, from prescriptions for birth control, STI testing, to prescription skin care and over-the-counter products. Favor’s most popular products are birth control (from over 120 brands), emergency contraception (“morning-after-pill”), STI (sexually transmitted infection) kits, condoms, and acne medications.

65. Before a customer can obtain a prescription for birth control from Favor, they must first create an account and answer an extensive medical history questionnaire encompassing a series

of sensitive, health-related questions, in addition to providing other health-related information. The questions include: (1) “what type of birth control are you on?”; (2) “are you pregnant?”; (3) “how long has it been since you last gave birth?”; (4) “how frequently would you like your period?”; (5) “are you taking hormones?”; (6) “are you breast feeding?”; (7) “are you menopausal?”; (8) “do you have history of breast cancer?”; (9) “do you have high cholesterol?”; (10) “select what other medications are you on?”; (11) “what is your blood pressure range?”; (12) “do you have heart disease?”; (13) “do you have hypertension?”, and many more.

The screenshot shows a web form titled "Favor" for a "Medical Consultation". It is the second of three steps, as indicated by a progress bar and the text "2 of 3". The question is "Are you taking any of these medications or supplements?" with the instruction "Please select all that apply." Below the question are three checkboxes, each with a medication name and a help icon (a question mark in a circle):

- Rifampin or Rifabutin, e.g. Rifadin, Mycobutin ? ☐
- Certain Anticonvulsants (including topiramate and lamotrigine) ? ☐
- Barbiturates ? ☐

66. Likewise, a customer seeking emergency contraception must answer questions including: (1) “what type of birth control do you use currently?”; (2) whether you are currently pregnant or breastfeeding; (3) what medications you take; (4) “do you have any medication allergies?”; and (5) “are you allergic to corn-containing products or food dye?”.

67. As another example, to get a prescription for acne medication, a customer must answer questions including: (1) “what are your skincare goals?”; (2) “where do you have acne?”; (3) “at what age did you start having acne?”; (4) “how would you describe your skin?”; (5) “is the skin on your face sensitive?”; (6) “do you have eczema?”; (7) “do you have rosacea?”; (8) “do you have a suspicious lesion on your face that you are concerned about?”; (9) “have you ever used any medication (prescription or over-the-counter) on your face?”; (10) “do you have any active ingredients and strengths you’re interested in for treating acne?”; (11) “are you okay to experience

1 some skin peeling and skin irritation at the beginning of your treatment?"; (12) whether you are  
 2 currently pregnant or breastfeeding; (13) "do you have any allergies?"; and (14) whether you have  
 3 any medical conditions, are taking any medications, or have had any surgeries.

4 68. Once the questionnaire is completed, the user is paired with a member of Favor's  
 5 Medical Team, consisting of doctors and nurse practitioners, licensed in the users' state. The doctor  
 6 or nurse practitioner "review [the users'] health history" and questionnaire results before prescribing  
 7 medication based on the individual's needs if "medically appropriate." Favor also has registered  
 8 nurses who are available to answer any medical-related questions a customer may have.

9 69. Favor's Pharmacy Team, encompassing pharmacists, intern pharmacists, and  
 10 pharmacy technicians, then review and process the prescription. Favor accepts most health insurance  
 11 policies and Medicaid and offers cash pricing to those that are uninsured.

12 70. After the prescription is received, members of Favor's Patient Care Team are  
 13 available to answer any additional questions the user may have relating to the prescription, side  
 14 effects, or treatment plan.

15 71. In addition to providing medical care and prescriptions, Favor also offers over-the-  
 16 counter sexual and reproductive healthcare products and skincare. Users can purchase condoms,  
 17 female condoms, pregnancy tests, and moisturizers, among other products.

18 72. Favor also provides medical information to individuals through its blog, which  
 19 contains a variety of articles relating to sexual wellness, reproductive health, medication, and side  
 20 effects to certain products. For instance, Favor features an article on its website "What Birth Control  
 21 is best for PCOS?" (polycystic ovary syndrome) and another titled "Bleeding After Plan B:  
 22 Causes & Side Effects."

### 23 **B. Favor's Promises to Users & Sharing of Data**

24 73. Favor pledges to users that it "takes the privacy of [users'] data and information very  
 25 seriously" and that "[a]ll of the information [Favor] hold[s] is *treated as Protected Health*  
 26 *Information (PHI).*" Accordingly, users' "data is held to *even stricter privacy standard* than  
 27 required by CCPA (Health Insurance Portability and Accountability Act ("HIPAA"), California  
 28 Confidentiality of Medical Information Act, Texas Medical Privacy Act, as some examples.)"

74. Favor promises users that it does not disclose to third parties, including analytics companies, *any* “personal information.” Favor claims the only information it shares is “aggregated” and “non-identifying” and that third parties cannot use information “for their commercial purposes.”

75. It then states it all bold and capital letters “WE DO NOT SELL OR MARKET YOUR PERSONAL INFORMATION AT ANY TIME.”

76. Given these representations and the types of services Favor provides, users like Plaintiff and Class members expected their data, including health information, and other interactions on the Favor website, to remain confidential.

77. Despite these promises, Defendants’ tracking technology was incorporated on the Favor Platform, through which Defendants intercepted highly sensitive personal and medical information Plaintiff and Class members entered on the Favor Platform, including their PII, prescriptions, answers to health questions (described above), medication side effects, allergies, age, and weight.

78. With respect to FullStory, it intercepted *all of the users’ interactions* on the Favor Platform—i.e., every click, tap, scroll, mouse movement and keystroke—including the highly sensitive medical information users entered into the Favor Platform when seeking treatment.

### C. TikTok’s Tracking Technology on the Favor Platform

79. TikTok has more than 750 million monthly users worldwide and is one of the top five largest social media companies. TikTok’s main source of revenue is selling ads, with reports showing that TikTok’s ad revenue for this year alone surpassed \$12 billion.

80. TikTok’s parent company reports similar growth with its advertising revenue increasing year to year, jumping from just \$7.3 billion in 2018 to \$38.6 billion by 2021.

Year	Total Revenue	Ad Revenue	% Ad Revenue
2021	\$58 billion	\$38.6 billion	66%
2020	\$34.4 billion	\$30 billion	87%
2019	\$17.15 billion	\$16.5 billion	96%
2018	\$7.4 billion	\$7.3 billion	98%

1           81. To increase its advertising revenue, TikTok offers tracking and analytics services,  
2 including the TikTok Pixel. More than a million websites, including Favor, incorporate the TikTok  
3 Pixel.

4           82. The TikTok Pixel is a piece of HTML code placed on a website that tracks users'  
5 interactions, including what pages they view, buttons they click on, and information they enter,  
6 along with a unique identifier.

7           83. The TikTok Pixel intercepts these communications immediately after they are sent  
8 and before they are received by the website operator.

9           84. In addition, the TikTok Pixel collects identifiable information such as the users' IP  
10 address, the device make, model, and operating system, browser information, a unique session ID,  
11 and first and third party cookie data that can be associated with a specific user.

12           85. TikTok uses the cookies it collects and/or its "Advanced Matching" feature to  
13 "recognize and learn about people from [the] website and the types of actions they do or don't take."  
14 In April 2022, TikTok made its collection of first- and third-party cookies automatic across all  
15 websites that incorporated the TikTok Pixel prior to March 10, 2022.

16           86. Once the TikTok Pixel intercepts this data, it is sent to TikTok's server, where it is  
17 stored and processed. The data collected by TikTok is then used to match website actions to  
18 individuals, as well as provide attribution reports and track users. Further, if the user has a TikTok  
19 account, the data is used in connection with TikTok's advertising services.

20           87. The TikTok Pixel is incorporated on the Favor Platform. Through this technology,  
21 TikTok intercepted Favor users' interactions with the Favor Platform, including personal  
22 information. As a result, information Plaintiff Jane Doe provided to Favor to obtain birth control,  
23 emergency contraception, and condoms was intercepted by TikTok.

24           88. Plaintiff Jane Doe did not consent to the interception of her data by TikTok.  
25 TikTok's interception of Plaintiff Jane Doe's sensitive data without her consent is an invasion of  
26 privacy and violates several laws, including the California Confidentiality of Medical Information  
27 Act ("CMIA") and the California Invasion of Privacy Act ("CIPA").  
28



**D. Meta’s Tracking Technology on the Favor Platform**

89. Meta is one of the largest advertising companies in the country. To date, Meta generates nearly 98% of its revenue through advertising bringing in a grand total of \$114.93 billion.

90. Meta’s advertising business began back in 2007 with the creation of “Facebook Ads,” which was marketed as a “completely new way of advertising online” that would allow “advertisers to deliver more tailored and relevant ads.”

91. Today, Meta provides advertising on its own platforms, such as Facebook and Instagram, as well as websites outside these apps through the Facebook Audience Network. Facebook alone has more than 2.9 billion active users.<sup>1</sup>

92. Meta’s advertising business has been extremely successful due, in large part, to Meta’s ability to target people at a granular level. “Among many possible target audiences, [Meta] offers advertisers,” for example, “1.5 million people ‘whose activity on Facebook suggests that they’re more likely to engage with/distribute liberal political content’ and nearly seven million Facebook users who ‘prefer high-value goods in Mexico.’”

93. Given the highly specific data used to target specific users, it is no surprise that millions of companies and individuals utilize Meta’s advertising services. Meta generates substantially all of its revenue from selling advertisement placements:

Year	Total Revenue	Ad Revenue	% Ad Revenue
2021	\$117.93 billion	\$114.93 billion	97.46%
2020	\$85.97 billion	\$84.17 billion	97.90%
2019	\$70.70 billion	\$69.66 billion	98.52%
2018	\$55.84 billion	\$55.01 billion	98.51%

94. One of Meta’s most powerful advertising tools is the Meta Pixel, formerly known as the Facebook Pixel, which launched in 2015 and its software development kit (SDK).

95. Meta touted the Meta Pixel as “a new way to report and optimize for conversions, build audiences and get rich insights about how people use your website.” According to Meta, to use the Meta Pixel an advertiser need only “place a single pixel across [its] entire website to report and optimize for conversions” so that the advertiser could “measure the effectiveness of [its]

<sup>1</sup><https://www.statista.com/statistics/264810/number-of-monthly-active-facebook-users-worldwide/>

1 advertising by understanding the action people take on [its] website.” The Meta Pixel is incorporated  
2 on 6.7 million websites, including Favor’s website.

3 96. Similar to the TikTok Pixel, the Meta Pixel is a snippet of code embedded on a third-  
4 party website that tracks a users’ activity as the users navigate through a website. As soon as a user  
5 takes any action on a webpage that includes the Meta Pixel, the code embedded in the page re-directs  
6 the content of the user’s communication to Meta while the exchange of the communication between  
7 the user and website provider is still occurring.

8 97. Through this technology, Meta intercepts each page a user visits, what buttons they  
9 click, as well as specific information they input into the website and what they searched. The Meta  
10 Pixel sends each of these pieces of information to Meta with other identifiable information, such as  
11 the users IP address. Meta stores this data on its own server, in some instances, for years on end.

12 98. This data is often associated with the individual users’ Facebook account. For  
13 example, if the user is logged into their Facebook account when the user visits Favor’s website,  
14 Meta receives third party cookies allowing Meta to link the data collected by the Meta Pixel to the  
15 specific Facebook user.

16 99. Meta can also link the data to a specific user through the “Facebook Cookie.” The  
17 Facebook Cookie is a workaround to recent cookie-blocking techniques, including one developed  
18 by Apple, Inc., to track users, including Facebook users.

19 100. Lastly, Meta can link user data to individual users through identifying information  
20 collected through the Meta Pixel through what Meta calls “Advanced Matching.” There are two  
21 forms of Advanced Matching: manual matching and automatic matching. Using Manual Advanced  
22 Matching the website developer manually sends data to Meta to link users. Using Automatic  
23 Advanced Matching, the Meta Pixel scours the data it receives to search for recognizable fields,  
24 including name and email address to match users to their Facebook accounts.

25 101. Importantly, even if the Meta Pixel collects data about a non-Facebook user, Meta  
26 still retains and uses the data collected through the Meta Pixel in its analytics and advertising  
27 services. These non-users are referred to as having “shadow profiles” with Meta.

28

1           102. At the time Plaintiff Jane Doe used the Favor Platform, she maintained active  
2 Facebook and Instagram accounts. Plaintiff Jane Doe accessed the Favor Platform from the same  
3 device she used to visit Facebook and Instagram, and Meta associated the data it collected about her  
4 from the Favor Platform with her Facebook and Instagram accounts.

5           103. Meta offers an analogous mobile version of the Meta Pixel known as a software  
6 development kit (SDK) to app developers. Meta's SDK allows app developers "to track events, such  
7 as a person installing your app or completing a purchase." By tracking these events developers can  
8 measure ad performance and build audiences for ad targeting.

9           104. Meta's SDK collects three types of App Events. Automatically Logged Events "logs  
10 app installs, app sessions, and in-app purchases." Standard Events are "popular events that Facebook  
11 has created for the app." Custom Events are "events [the app developer] create that are specific to  
12 [the] app."

13           105. Once the data intercepted through the Meta Pixel or SDK is processed, Meta makes  
14 this data available through its Events Manager, along with tools and analytics to reach these  
15 individuals through future Facebook ads. For instance, this data can be used to create "custom  
16 audiences" to target the user, as well as other Facebook users who match members' of the audiences'  
17 criteria.

18           106. In addition to using the data intercepted through the Meta Pixel and the SDK to  
19 provide analytics services, Meta uses this data to improve its personalized content delivery,  
20 advertising network, and machine-learning algorithms, including by improving its ability to identify  
21 and target users.

22           107. Meta has no way to limit or prohibit the use of data collected through the Meta Pixel  
23 and its SDK given Meta's open systems and advanced algorithms.

24           108. According to leaked internal Meta documents, one employee explained "You pour  
25 that ink [i.e., data] into a lake of water . . . and it flows . . . everywhere . . . How do you put that ink  
26 back in the bottle? How do you organize it again, such that it only flows to the allowed places in the  
27 lake?"  
28

1           109. In these same leaked documents, another employee explained Meta does “not have  
2 an adequate level of control and explainability over how our systems use data, and thus we can’t  
3 confidently make controlled policy changes or external commitments such as ‘we will not use X  
4 data for Y purpose.’ And yet, that is exactly what regulators expect us to do, increasing our risk of  
5 mistakes and misrepresentation.” Thus, once the data enters the Meta system, either through its SDK  
6 or Pixel, the data can be used for any and all purposes.

7           110. Meta’s own employees confirmed no one at Meta can state confidently where all the  
8 data about a user is stored and used. In a recent court hearing as part of the Cambridge Analytica  
9 scandal of 2018, Meta’s own engineers testified there was not a “single person” at Meta who could  
10 answer that question.

11           111. The Meta Pixel and SDK are incorporated on the Favor Platform. As a result, Meta  
12 intercepted users’ interactions on the Favor Platform. For instance, Meta received users’ specific  
13 responses to medical history and other health questions Favor asked in connection with a visit for  
14 birth control. This included highly sensitive medical information as reflected in paragraphs 4-6, 13,  
15 65-68 above.

16           112. Plaintiff Jane Doe provided her PII, health information, and other sensitive data to  
17 Favor to obtain birth control, emergency contraception, and condoms, this information was sent to  
18 Meta.

19           113. Plaintiff Jane Doe did not consent to the interception of her data by Meta. Meta’s  
20 interception of Plaintiff Jane Doe’s PII, health data, and other highly sensitive information without  
21 her consent is an invasion of privacy and violates several laws, including the CMIA and CIPA.

#### 22           **E. FullStory and Session Replay**

23           114. FullStory was founded in 2014 and is a data analytics company that offers a variety  
24 of products, from data collection to analytics. The company raised close to \$170 million in funding  
25 and is valued at over \$1.5 billion as of August 4, 2021.

26           115. FullStory is one of the leading session replay companies in the market today, touting  
27 its capabilities as “a modern way to collect user experience data” where “the amount of valuable  
28 information FullStory captures is second to none . . . .”

1           116. According to FullStory, “A website represents thousands and thousands of UX [user  
2 experience] decisions, and with FullStory [they] can ‘watch’ sessions and frequently uncover  
3 opportunities.”

4           117. FullStory “watch[es] sessions” through sophisticated session replay code that runs in  
5 the background of any given website or mobile application. Its session replay code makes a  
6 “detailed accounting of every action that takes place on [the] site or app. From mouse movements  
7 and clicks to screen swipes or typing.” Each of these pieces of data are bundled, transmitted, and  
8 then “store[d] and organize[d]” by FullStory on their platform, along with a unique identifier (i.e.,  
9 UserID and SessionID) for each particular user whose communications they intercept.

10           118. As a result, website visitors’ interactions with and communications on websites that  
11 incorporate this software, like the Favor Platform, are intercepted by FullStory in real-time.

12           119. Once this data is intercepted, FullStory provides a dashboard platform that provides  
13 its clients “access [to] data that’s automatically indexed, fully retroactive, and instrumentation-free  
14 to get insight into all digital interactions.” On FullStory’s dashboard, its clients are able to filter the  
15 sessions and identify users based on their actions on the site.

16           120. Not only does FullStory intercept vast amounts of data from its clients’ websites, it  
17 also leverages that data to provide analytics insights such as factors impacting the sites conversions  
18 and device-specific bugs. It also supplies custom conversion analyses using its “extensive searchable  
19 data.”

20           121. While FullStory claims that it “requires users to block sensitive information from  
21 being recorded,” it does not have the capability to do so and does not enforce that policy. As  
22 explained in paragraphs 47-49 above, researchers have shown that FullStory’s “automated redaction  
23 process,” which purportedly prevents sensitive information like health data from being recorded,  
24 does not successfully remove that data.

25           122. FullStory’s session replay software is incorporated on the Favor Platform. As a  
26 result, FullStory intercepted each of its users’ interactions on the Favor Platform along with a unique  
27 ID that can individually identify the user. For instance, FullStory received users’ type of medication,  
28 side effects, and allergies, as well as other responses to health questions. Thus, if a user previously

1 used a birth control with side effects, FullStory intercepted this information along with the name of  
2 the medication.

3 123. Plaintiff Jane Doe provided her PII, health information, and other sensitive data to  
4 Favor to obtain birth control, emergency contraception, and condoms, this information was  
5 intercepted by FullStory.

6 124. Plaintiff Jane Doe did not consent to the interception of her data by FullStory.  
7 FullStory's interception of Plaintiff Jane Doe's PII, health data, and other highly sensitive  
8 information without her consent is an invasion of privacy and violates several laws, including the  
9 CMIA and CIPA.

#### 10 **F. Plaintiff and Class Members Do Not Consent to Defendants' Conduct**

11 125. Plaintiff and Class members had no way of knowing that Defendants were  
12 intercepting their communications when interacting with the Favor Platform because their software  
13 is inconspicuously incorporated in the background.

14 126. This conduct is all the more egregious given the nature of the information entered  
15 into the Favor Platform, e.g., PII, requests for prescriptions, and identifiable medical information,  
16 among other things. Plaintiff and Class members would not expect this information to be intercepted  
17 without their consent.

18 127. This is especially true given Favor's consistent representations that this information  
19 would remain private and confidential. Favor promises that it "takes the privacy of [users'] data and  
20 information very seriously" and that "[a]ll of the information [Favor] hold[s] is ***treated as Protected***  
21 ***Health Information (PHI)***." Accordingly, users' "data is held to ***even stricter privacy standard***  
22 than required by CCPA (Health Insurance Portability and Accountability Act ("HIPAA"), California  
23 Confidentiality of Medical Information Act, Texas Medical Privacy Act, as some examples.)"

24 128. It later states that it "understand[s] that medical information about [users] and [their]  
25 health is personal" and that Favor is "committed to protecting it" and, further, that no "personal  
26 information" would be intercepted by third parties, including analytics companies.

27 129. Doubling down, it then states in all bold and capital letters, Favor ensures users "WE  
28 DO NOT SELL OR MARKET YOUR PERSONAL INFORMATION AT ANY TIME." It claims

1 that it only discloses “aggregated” and “non-identifying” information and, even then, that third  
 2 parties cannot use information “for their commercial purposes.”

3 130. Favor repeats these assurances throughout its privacy policy, stating that it is  
 4 “required by law to make sure that medical information which identifies [users] is kept private (with  
 5 certain exceptions).” These “exceptions” include the disclosure of users’ information for things like  
 6 treatment and law enforcement needs and do not include the disclosure of users’ information for  
 7 marketing, advertising, tracking, or analytics purposes to companies like Defendants.

8 131. Accordingly, Plaintiff and Class members did not consent to Defendants’ conduct.

9 **G. Plaintiff and Class Members have a Reasonable Expectation of Privacy in their**  
 10 **User Data**

11 132. Plaintiff and Class members have a reasonable expectation of privacy in their  
 12 communications on the Favor Platform, including their health information.

13 133. Privacy polls and studies uniformly show that the overwhelming majority of  
 14 Americans consider one of the most important privacy rights to be the need for an individual’s  
 15 affirmative consent before a company collects and shares its customers’ personal data.

16 134. For example, a recent study by *Consumer Reports* shows that 92% of Americans  
 17 believe that internet companies and websites should be required to obtain consent before selling or  
 18 sharing consumers’ data, and the same percentage believe internet companies and websites should  
 19 be required to provide consumers with a complete list of the data that has been collected about them.  
 20 Moreover, according to a study by *Pew Research Center*, a majority of Americans, approximately  
 21 79%, are concerned about how data is collected about them by companies.

22 135. Users act consistent with these preferences. Following a new rollout of the iPhone  
 23 operating software—which asks users for clear, affirmative consent before allowing companies to  
 24 track users—85% of worldwide users and 94% of U.S. users chose not to share data when prompted.

25 136. Another recent study by DataGrail revealed that 67% of people were willing to pay  
 26 \$100 or more annually to keep their information out of the hands of companies and the government.  
 27 The same study revealed that 75% of people would abandon brands that do not take care of their  
 28 data.



1           137. Other privacy law experts have expressed concerns about the disclosure to third  
 2 parties of a users’ intimate health data. For example, Dena Mendelsohn—the former Senior Policy  
 3 Counsel at Consumer Reports and current Director of Health Policy and Data Governance at Elektra  
 4 Labs—explained that having your personal health information disseminated in ways you are  
 5 unaware of could have serious repercussions, including affecting your ability to obtain life insurance  
 6 and how much you pay for that coverage, increase the rate you’re charged on loans, and leave you  
 7 vulnerable to workplace discrimination.

8           138. This data is also extremely valuable. According to Experian, health data is a “gold  
 9 mine” for healthcare companies and clinicians.

10           139. Consumers’ health data, including what prescriptions they have, are extremely  
 11 profitable. For instance, Datarade.ai advertises access to U.S. customers names, addresses, email  
 12 addresses, telephone numbers who bought brand name medicine. The starting price for access to  
 13 just some of this data was \$10,000. Other companies, like Pfizer, spend \$12 million annually to  
 14 purchase health data and the medical data industry itself was valued at over \$2.6 billion back in  
 15 2014.

16           140. Defendants’ surreptitious interception of Plaintiff’s and Class members’ private  
 17 communications, including PII, health information, and other sensitive data violates Plaintiff’s and  
 18 Class members’ privacy interests.

### 19                           **TOLLING, CONCEALMENT, AND ESTOPPEL**

20           141. The applicable statutes of limitation have been tolled as a result of Defendants’  
 21 knowing and active concealment and denial of the facts alleged herein.

22           142. Defendants’ software was secretly incorporated into the Favor Platform, providing  
 23 no indication to users that they were interacting with sites that shared their data, including PII and  
 24 medical information, with third parties.

25           143. Defendants had exclusive knowledge that the Favor Platform incorporated its  
 26 software, yet failed to disclose that fact to users, or that by interacting with the Favor Platform,  
 27 Plaintiff’s and Class members’ sensitive data, including PII and health data, would be intercepted  
 28 by third parties.

144. Plaintiff and Class members could not with due diligence have discovered the full scope of Defendants' conduct, including because it is highly technical and there were no disclosures or other indication that would inform a reasonable consumer that third parties, including Defendants, were intercepting, data from the Favor Platform.

145. The earliest Plaintiff and Class members could have known about Defendants' conduct was shortly before the filing of this Complaint.

146. Defendants were under a duty to disclose the nature and significance of their data collection practices but did not do so. Defendants are therefore estopped from relying on any statute of limitations under the discovery rule.

147. Additionally, Defendants engaged in fraudulent conduct to prevent Plaintiff and Class members from discovering the interception of their data. Favor misled Plaintiff and Class members to believe their data, including health information and PII, would not be intercepted.

148. Favor represented to Plaintiff and Class members that they applied even stronger restrictions on the sharing of data than those imposed by HIPAA and the CMIA. It also promised Plaintiff and Class members that their "personal information" would not be shared. No Defendant disclosed the misconduct alleged herein.

149. Plaintiff and Class members were not aware that Defendants intercepted their data, including PII and health information.

150. Plaintiff and Class members exercised due diligence to uncover the facts alleged herein and did not have actual or constructive knowledge of Defendants' misconduct by virtue of their fraudulent concealment.

151. Accordingly, all statute of limitations are tolled under the doctrine of fraudulent concealment.

#### **CLASS ACTION ALLEGATIONS**

152. Plaintiff brings this action pursuant to Federal Rule of Civil Procedure 23 individually and on behalf of the following Class:

**Nationwide Class:** All natural persons in the United States who used the Favor Platform and whose communications and/or data were intercepted by Defendants.

153. Excluded from the Class are: (1) any Judge or Magistrate presiding over this action and any members of their immediate families; (2) the Defendants, Defendants' subsidiaries, affiliates, parents, successors, predecessors, and any entity in which the Defendants or their parents have a controlling interest and their current or former employees, officers, and directors; and (3) Plaintiff's counsel and Defendants' counsel.

154. **Numerosity:** The exact number of members of the Class is unknown and unavailable to Plaintiff at this time, but individual joinder in this case is impracticable. The Class likely consists of millions of individuals, and the members can be identified through Favor's records.

155. **Predominant Common Questions:** The Class' claims present common questions of law and fact, and those questions predominate over any questions that may affect individual Class members. Common questions for the Class include, but are not limited to, the following:

- Whether Defendants violated Plaintiff's and Class members' privacy rights;
- Whether Defendants' acts and practices violated the Common Law Invasion of Privacy;
- Whether Defendants were unjustly enriched;
- Whether Defendants' acts and practices violated California's Confidentiality of Medical Information Act, Civil Code §§ 56, *et seq.*;
- Whether Defendants' acts and practices violated the California Invasion of Privacy Act, Cal. Penal Code §§ 630, *et seq.*;
- Whether Plaintiff and the Class members are entitled to equitable relief, including, but not limited to, injunctive relief, restitution, and disgorgement; and
- Whether Plaintiff and the Class members are entitled to actual, statutory, punitive or other forms of damages, and other monetary relief.

156. **Typicality:** Plaintiff's claims are typical of the claims of the other members of the Class. The claims of Plaintiff and the members of the Class arise from the same conduct by Defendants and are based on the same legal theories.

157. **Adequate Representation:** Plaintiff has and will continue to fairly and adequately represent and protect the interests of the Class. Plaintiff has retained counsel competent and

1 experienced in complex litigation and class actions, including litigations to remedy privacy  
 2 violations. Plaintiff has no interest that is antagonistic to the interests of the Class, and Defendants  
 3 have no defenses unique to any Plaintiff. Plaintiff and their counsel are committed to vigorously  
 4 prosecuting this action on behalf of the members of the Class, and they have the resources to do so.  
 5 Neither Plaintiff nor their counsel have any interest adverse to the interests of the other members of  
 6 the Class.

7       158. **Substantial Benefits:** This class action is appropriate for certification because class  
 8 proceedings are superior to other available methods for the fair and efficient adjudication of this  
 9 controversy and joinder of all members of the Class is impracticable. This proposed class action  
 10 presents fewer management difficulties than individual litigation, and provides the benefits of single  
 11 adjudication, economies of scale, and comprehensive supervision by a single court. Class treatment  
 12 will create economies of time, effort, and expense and promote uniform decision-making.

13       159. Plaintiff reserves the right to revise the foregoing class allegations and definitions  
 14 based on facts learned and legal developments following additional investigation, discovery, or  
 15 otherwise.

#### 16                   **CALIFORNIA LAW APPLIES TO THE ENTIRE CLASS**

17       160. California substantive laws apply to every member of the Class. California's  
 18 substantive laws may be constitutionally applied to the claims of Plaintiff and the Classes under the  
 19 Due Process Clause, 14th Amend. § 1, and the Full Faith and Credit Clause, Art. IV. § 1 of the U.S.  
 20 Constitution. California has significant contact, or significant aggregation of contacts, to the claims  
 21 asserted by Plaintiff and Class members, thereby creating state interests to ensure that the choice of  
 22 California state law is not arbitrary or unfair.

23       161. Meta and TikTok maintain their principal places of business in California and  
 24 conduct substantial business in California, such that California has an interest in regulating Meta  
 25 and TikTok's conduct under its laws. Meta also selected California law as the law to govern all  
 26 disputes with their customers in their respective terms of service. Defendants Meta and TikTok's  
 27 decision to reside in California and avail themselves of California's laws renders the application of  
 28 California law to the claims herein constitutionally permissible.

162. The application of California laws to the Class is also appropriate under California's choice of law rules because California has significant contacts to the claims of Plaintiff and the proposed Class, and California has a greater interest in applying its laws here given Defendants' locations and the location of the conduct at issue than any other interested state.

### **CLAIMS FOR RELIEF**

#### **FIRST CLAIM FOR RELIEF**

#### **Violation of Common Law Invasion of Privacy – Intrusion Upon Seclusion (On Behalf of the Plaintiff and the Class) (Against all Defendants)**

163. Plaintiff re-alleges and incorporates the preceding allegations of this Complaint with the same force and effect as if fully restated herein.

164. A Plaintiff asserting claims for intrusion upon seclusion must plead (1) that the defendant intentionally intruded into a place, conversation, or matter as to which Plaintiff have a reasonable expectation of privacy; and (2) that the intrusion was highly offensive to a reasonable person.

165. Defendants' surreptitious interception, storage, and use of Plaintiff's and Class members' interactions and communications with the Favor Platform, including PII, health information, and prescription requests, constitutes an intentional intrusion upon Plaintiff's and Class members' solitude or seclusion.

166. Plaintiff and Class members expected this information to remain private and confidential given the nature of the Favor Platform, which is primarily used to receive medical advice, treatment, and prescriptions.

167. This expectation is especially heightened given Favor's consistent representations that this data would remain confidential. Plaintiff and Class members did not expect third parties, and specifically Defendants, to secretly intercept this information and their communications.

168. Plaintiff and Class members did not consent to, authorize, or know about Defendants' intrusion at time it occurred. Plaintiff and Class members never agreed that Defendants could intercept, store, and use this data.

1           169. Defendants' intentional intrusion on Plaintiff's and Class members' solitude or  
2 seclusion would be highly offensive to a reasonable person. Plaintiff and Class members reasonably  
3 expected, based on Favor's repeated assurances, that their information would not be collected by  
4 Defendants.

5           170. The surreptitious taking and interception of sensitive data, including PII and medical  
6 information, from millions of individuals was highly offensive because it violated expectations of  
7 privacy that have been established by social norms. Privacy polls and studies show that the  
8 overwhelming majority of Americans believe one of the most important privacy rights is the need  
9 for an individual's affirmative consent before personal data is collected or shared.

10           171. The offensiveness of this conduct is all the more apparent because Defendants'  
11 interception, storage, and use of this information was conducted inconspicuously in a manner that  
12 Plaintiff and Class members would be unable to detect and was contrary to the actual representations  
13 made by Favor.

14           172. Given the highly sensitive nature of the data that Defendants intercepted, such as  
15 private details about medications and health information, this kind of intrusion would be (and in fact  
16 is) highly offensive to a reasonable person.

17           173. As a result of Defendants' actions, Plaintiff and Class members have suffered harm  
18 and injury, including, but not limited to, an invasion of their privacy rights.

19           174. Plaintiff and Class members have been damaged as a direct and proximate result of  
20 Defendants' invasion of their privacy and are entitled to just compensation, including monetary  
21 damages.

22           175. Plaintiff and Class members seek appropriate relief for that injury, including but not  
23 limited to damages that will reasonably compensate Plaintiff and Class members for the harm to  
24 their privacy interests as well as a disgorgement of profits made by Defendants as a result of its  
25 intrusions upon Plaintiff's and Class members' privacy.

26           176. Plaintiff and Class members are also entitled to punitive damages resulting from the  
27 malicious, willful, and intentional nature of Defendants' actions, directed at injuring Plaintiff and  
28

1 Class members in conscious disregard of their rights. Such damages are needed to deter Defendants  
2 from engaging in such conduct in the future.

3 177. Plaintiff also seeks such other relief as the Court may deem just and proper.

4 **SECOND CLAIM FOR RELIEF**  
5 **Unjust Enrichment**  
6 **(On Behalf of Plaintiff and the Class)**  
7 **(Against all Defendants)**

8 178. Plaintiff re-alleges and incorporates the preceding allegations of this Complaint with  
9 the same force and effect as if fully restated herein.

10 179. Defendants received benefits from Plaintiff and Class members and unjustly retained  
11 those benefits at their expense.

12 180. Defendants received benefits from Plaintiff and Class members in the form of the  
13 Plaintiff's and Class members' highly valuable data, including health information and PII, that  
14 Defendants wrongfully intercepted from Plaintiff and Class members without authorization and  
15 proper compensation.

16 181. Defendants intercepted, stored, and used this data for their own gain, providing  
17 Defendants with economic, intangible, and other benefits, including highly valuable data for  
18 analytics, advertising, and improvement of their platforms, algorithms, and advertising services.

19 182. Had Plaintiff known of Defendants' misconduct, she would not have provided any  
20 of her data to Defendants or used the Favor Platform.

21 183. Defendants unjustly retained these benefits at the expense of Plaintiff and Class  
22 members because Defendants' conduct damaged Plaintiff and Class members, all without providing  
23 any commensurate compensation to Plaintiff and Class members.

24 184. The benefits that Defendants derived from Plaintiff and Class members rightly  
25 belong to Plaintiff and Class members. It would be inequitable under unjust enrichment principles  
26 in California and every other state for Defendants to be permitted to retain any of the profit or other  
27 benefits they derived from the unfair and unconscionable methods, acts, and trade practices alleged  
28 in this Complaint.



185. Defendants should be compelled to disgorge in a common fund for the benefit of Plaintiff and Class members all unlawful or inequitable proceeds that Defendants received, and such other relief as the Court may deem just and proper.

**THIRD CLAIM FOR RELIEF**  
**Violation of California Confidentiality of Medical Information Act (“CMIA”)**  
**Civil Code Section 56.36**  
**(On Behalf of Plaintiff and the Class)**  
**(Against all Defendants)**

186. Plaintiff re-alleges and incorporates the preceding allegations of this Complaint with the same force and effect as if fully restated herein.

187. California Civil Code Section 56.36(B)(3)(A) prohibits any person of entity other than a licensed health care professional from knowingly or willfully obtaining medical information for financial gain.

188. California Civil Code Section 56.36(B)(5) prohibits any person or entity who is not permitted to receive medical information under the CMIA from knowingly and willfully obtaining, disclosing, or using the medical information without written authorization.

189. Defendants are entities who are not licensed health care professionals, and Defendants are not permitted to receive medical information under the CMIA.

190. Defendants violated California Civil Code Section 56.36(B)(3)(A) and (B)(5) because they knowingly and willfully obtained medical information from the Favor Platform without authorization for their own financial gain.

191. As described herein, Defendants intentionally designed their software, i.e., the Meta Pixel and SDK, TikTok Pixel, and FullStory’s session replay software, to intercept data from the websites and mobile applications in which they are incorporated.

192. Defendants knew this software was incorporated on websites and mobile applications that would consequently lead to the interception of medical information, including medical information input in the Favor Platform.

193. Defendants knowingly and willfully received this information without written authorization from Plaintiff and Class members and did so for their own financial gain. Namely, to

1 profit through advertising and analytics services they offer, as well as to improve their algorithms,  
2 data points, and other technologies.

3 194. Pursuant to California Civil Code Section 56.36(B)(3)(A) and California Civil Code  
4 Section 56.36(B)(5), Defendants are liable for a civil penalty up to \$250,000 per violation of these  
5 sections.

6 **FOURTH CLAIM FOR RELIEF**  
7 **Violation of the California Invasion of Privacy Act (“CIPA”)**  
8 **Cal. Penal Code § 631**  
9 **(On Behalf of Plaintiff and the Class and Subclass)**  
10 **(Against all Defendants)**

11 195. Plaintiff re-alleges and incorporates the preceding allegations of this Complaint with  
12 the same force and effect as if fully restated herein.

13 196. The California Legislature enacted the California Invasion of Privacy Act, Cal. Penal  
14 Code §§ 630, *et seq.* (“CIPA”) finding that “advances in science and technology have led to the  
15 development of new devices and techniques for the purpose of eavesdropping upon private  
16 communications and that the invasion of privacy resulting from the continual and increasing use of  
17 such devices and techniques has created a serious threat to the free exercise of personal liberties and  
18 cannot be tolerated in a free and civilized society.” *Id.* § 630. Thus, the intent behind CIPA is “to  
19 protect the right of privacy of the people of this state.” *Id.*

20 197. Cal. Penal Code § 631 imposes liability on any person who “by means of any  
21 machine, instrument, contrivance, or in any other manner” (1) “intentionally taps, or makes any  
22 unauthorized connection . . . with any telegraph or telephone wire, line, cable, or instrument,”  
23 (2) “willfully and without the consent of all parties to the communication, or in any unauthorized  
24 manner, reads or attempts to read, or to learn the contents or meaning of any message, report, or  
25 communication while the same is in transit or passing over any wire, line, or cable, or is being sent  
26 from, or received at any place within [the state of California],” (3) “uses, or attempts to use, in any  
27 manner, or for any purpose, or to communicate in any way, any information so obtained,” or  
28 (4) “aids, agrees with, employs, or conspires with any person or persons to unlawfully do, or permit,  
or cause to be done any of the acts or things mentioned above in this section.”

198. Defendants are persons for purposes of § 631.

1            199. Defendants Meta and TikTok maintain their principal places of business in  
2 California, where they designed, contrived, agreed, conspired, effectuated, and/or received the  
3 interception and use of the contents of Plaintiff's and Class members' communications.  
4 Additionally, Meta has adopted California substantive law to govern their relationship with users.

5            200. The Meta Pixel and SDK, the TikTok Pixel, and FullStory's session replay software,  
6 Plaintiff's and Class members' browsers and mobile applications, and Plaintiff's and Class  
7 members' computing and mobile devices are a "machine, instrument, contrivance, or . . . other  
8 manner."

9            201. At all relevant times, Meta, using its Meta Pixel and SDK, TikTok, using its TikTok  
10 Pixel, and FullStory, using its session replay software, intentionally tapped or made unauthorized  
11 connections with, the lines of internet communication between Plaintiff and Class members and the  
12 Favor Platform without the consent of all parties to the communication.

13            202. Defendants, willfully and without the consent of Plaintiff and Class members, reads  
14 or attempt to reads, or learn the contents or meaning of Plaintiff's and Class members'  
15 communications to Favor while the communications are in transit or passing over any wire, line or  
16 cable, or were being received at any place within California when it intercepted Plaintiff's and Class  
17 members' communications and data with Favor, who is headquartered in California, in real time.

18            203. Defendants used or attempted to use the communications and information they  
19 received through their pixels, SDK, and session replay technology, including to supply analytics  
20 and advertising services.

21            204. The interception of Plaintiff's and Class members' communications was without  
22 authorization and consent from the Plaintiff and Class members. Accordingly, the interception was  
23 unlawful and tortious.

24            205. Plaintiff and the Class members seek statutory damages in accordance with  
25 § 637.2(a), which provides for the greater of: (1) \$5,000 per violation; or (2) three times the amount  
26 of damages sustained by Plaintiff and the Class in an amount to be proven at trial, as well as  
27 injunctive or other equitable relief.  
28

206. Plaintiff and Class members have also suffered irreparable injury from these unauthorized acts. Plaintiff's and Class members' sensitive data has been collected, viewed, accessed, and stored by Defendants, has not been destroyed, and due to the continuing threat of such injury, Plaintiff and Class members have no adequate remedy at law, Plaintiff and Class members are entitled to injunctive relief.

**FIFTH CLAIM FOR RELIEF**  
**Violation of CIPA**  
**Cal. Penal Code § 632**  
**(On Behalf of Plaintiff and the Class and Subclass)**  
**(Against all Defendants)**

207. Plaintiff re-alleges and incorporates the preceding allegations of this Complaint with the same force and effect as if fully restated herein.

208. Cal. Penal Code § 632 prohibits "intentionally and without the consent of all parties to a confidential communication," the "use[] [of] an electronic amplifying or recording device to eavesdrop upon or record the confidential communication[.]"

209. Section 632 defines "confidential communication" as "any communication carried on in circumstances as may reasonably indicate that any party to the communication desires it to be confined to the parties thereto[.]"

210. Plaintiff's and Class members' communications to Favor, including their sensitive medical information including information concerning medications they were taking or were prescribed, their medical histories, allergies, and answers to other health-related questions, were confidential communications for purposes of § 632, including because Plaintiff and Class members had an objectively reasonable expectation of privacy in this data.

211. Plaintiff and Class members expected their communications to Favor to be confined to Favor, in part because of Favor's consistent representations that these communications would remain confidential. Plaintiff and Class members did not expect third parties, and specifically Defendants, to secretly eavesdrop upon or record this information and their communications.

212. The Meta Pixel and SDK, the TikTok Pixel, and FullStory's session replay software are all electronic amplifying or recording devices for purposes of § 632.

213. By contemporaneously intercepting and recording Plaintiff's and Class members' confidential communications to Favor through the Meta Pixel and SDK, the TikTok Pixel, and session replay software, Defendants eavesdropped and/or recorded confidential communications through an electronic amplifying or recording device in violation of § 632 of CIPA.

214. At no time did Plaintiff or Class members consent to Defendants' conduct, nor could they reasonably expect that their communications to Favor would be overheard or recorded by Defendants.

215. Defendants utilized Plaintiff's and Class members' sensitive medical information for their own purposes, including advertising and analytics.

216. Plaintiff and Class members seek statutory damages in accordance with § 637.2(a) which provides for the greater of: (1) \$5,000 per violation; or (2) three times the amount of damages sustained by Plaintiff and the Class in an amount to be proven at trial, as well as injunctive or other equitable relief.

217. Plaintiff and Class members have also suffered irreparable injury from these unauthorized acts. Plaintiff's and Class members' sensitive data has been collected, viewed, accessed, and stored by Defendants, has not been destroyed, and due to the continuing threat of such injury, Plaintiff and Class members have no adequate remedy at law, Plaintiff and Class members are entitled to injunctive relief.

#### **PRAYER FOR RELIEF**

WHEREFORE, Plaintiff on behalf of herself and the proposed Class respectfully requests that the Court enter an order:

- A. Certifying the Class and appointing Plaintiff as the Class' representative;
- B. Finding that Defendants' conduct was unlawful, as alleged herein;
- C. Awarding declaratory relief against Defendants;
- D. Awarding such injunctive and other equitable relief as the Court deems just and proper;

1 E. Awarding Plaintiff and the Class members statutory, actual, compensatory,  
2 consequential, punitive, and nominal damages, as well as restitution and/or disgorgement of profits  
3 unlawfully obtained;

4 F. Awarding Plaintiff and the Class members pre-judgment and post-judgment interest;

5 G. Awarding Plaintiff and the Class members reasonable attorneys' fees, costs, and  
6 expenses; and

7 H. Granting such other relief as the Court deems just and proper.

8 Dated: July 31, 2023

**LOWEY DANNENBERG, P.C.**

9 By: /s/ Christian Levis

10 Christian Levis (admitted *pro hac vice*)  
11 Amanda Fiorilla (admitted *pro hac vice*)  
12 Rachel Kesten (admitted *pro hac vice*)  
13 Christopher Devivo (*pro hac vice* forthcoming)  
14 44 South Broadway, Suite 1100  
15 White Plains, NY 10601  
16 Tel.: (914) 997-0500  
17 Fax: (914) 997-0035  
18 clevis@lowey.com  
19 afiorilla@lowey.com  
20 rkesten@lowey.com  
21 cdevivo@lowey.com

**LYNCH CARPENTER, LLP**

22 (Eddie) Jae K. Kim (CA Bar No. 236805)  
23 117 East Colorado Blvd., Suite 600  
24 Pasadena, CA 91105  
25 Tel.: (626) 550-1250  
26 ekim@lcllp.com

**LYNCH CARPENTER, LLP**

27 Gary F. Lynch (admitted *pro hac vice*)  
28 Jamisen A. Etzel (admitted *pro hac vice*)  
Nicholas A. Colella (admitted *pro hac vice*)  
1133 Penn Ave., 5th Floor  
Pittsburgh, PA 15222  
Tel.: (412) 322-9243  
gary@lcllp.com  
jamisen@lcllp.com  
nickc@lcllp.com

*Attorneys for Plaintiff and the Proposed Class*